**-LOGO-**

**-QURUM ADI-**

**TƏHDİD KƏŞFİYYATI SİYASƏTİ**

# SƏNƏDİN TARİXÇƏSİ

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Kod** | **Hazırlayan** | **Nəzərdən Keçirən** | **Təsdiqləyən/Təsdiq Tarixi** | **Versiya** | **Dəyişiklik Tarixi** | **Dəyişiklik Səbəbi** | **Məxfilik Səviyyəsi** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

MÜNDƏRİCAT

[SƏNƏDİN TARİXÇƏSİ 2](#_Toc188536442)

[1. ÜMUMİ MÜDDƏALAR 4](#_Toc188536443)

[2. ANLAYIŞLAR 4](#_Toc188536444)

[3. ƏHATƏ DAİRƏSİ 4](#_Toc188536445)

[4. MƏSULİYYƏTLƏR 5](#_Toc188536446)

[5. TƏTBİQ 6](#_Toc188536447)

[5.1. TƏHDİD KƏŞFİYYATININ İZAHI 6](#_Toc188536448)

[5.2. TƏHDİD KƏŞFİYYATININ TƏBƏQƏLƏRİ 6](#_Toc188536449)

[5.3. QURUMDA STRATEJİ KƏŞFİYYAT 6](#_Toc188536450)

[5.4. QURUMDA TAKTİKİ KƏŞFİYYAT 7](#_Toc188536451)

[5.5. QURUMDA ƏMƏLİYYAT KƏŞFİYYATI 7](#_Toc188536452)

[5.6. QURUMDA TEXNİKİ KƏŞFİYYAT 8](#_Toc188536453)

[6. ƏLAQƏLİ SƏNƏDLƏR 9](#_Toc188536454)

[7. İNTİZAM TƏDBİRLƏRİ 9](#_Toc188536455)

[8. SİYASƏTƏ NƏZARƏT 9](#_Toc188536456)

[TƏSDİQETMƏ 10](#_Toc188536457)

# ÜMUMİ MÜDDƏALAR

Təhdid kəşfiyyatı siyasətinin (bunda sonra- Siyasət) məqsədi “Qurum adı”-nın (bundan sonra- Qurum) informasiya təhlükəsizliyinin qorunması və dayanıqlığının artırılması üçün təhdid kəşfiyyatının effektiv şəkildə həyata keçirilməsini təmin etməkdir. Təhdid kəşfiyyatı prosesləri vasitəsilə potensial təhlükələrin vaxtında müəyyən edilməsi, qiymətləndirilməsi və onlara qarşı tədbirlərin görülməsi ilə bağlı çərçivə təqdim olunur.

Siyasət, qurumun informasiya aktivlərinə qarşı yönəlmiş təhdidlərin proaktiv şəkildə izlənməsi, məlumatların toplanması, təhlili və paylaşıması vasitəsilə risklərin azaldılmasını hədəfləyir. Bu, həmçinin qurumun hüquqi və tənzimləyici tələblərə uyğunluğunu təmin etməklə yanaşı, təhlükəsizlik üzrə qabaqlayıcı tədbirlərin tətbiqini dəstəkləyir.

Beləliklə, siyasət quruma aşağıdakıları təmin etməyi qarşıya məqsəd qoyur:

* İnformasiya təhlükəsizliyinə təhdid yaradan faktorların erkən aşkarlanması;
* Təhdidlərin təsirini azaltmaq üçün strategiyaların hazırlanması;
* Təhlükəsizlik məsələlərində məlumatlılığın artırılması və əməkdaşlıq mühitinin yaradılması.

# ANLAYIŞLAR

**IOC (Indicators of Compromise):** Haker hücumlarının izlərini göstərən texniki göstəricilər. Bunlara zərərli IP ünvanları, domenlər, fayl hash-ləri və qeyri-adi şəbəkə fəaliyyəti daxildir;

**Təhdid aktyoru:** Müəyyən bir məqsəd üçün quruma qarşı təhlükə yaradan şəxslər, qruplar və ya təşkilatlar. Bunlar daxili və ya xarici mənbələrdən ola bilər;

**Zəiflik:** Qurumun sistemlərində və ya proseslərində olan və potensial olaraq istismar edilə bilən zəif nöqtələr;

**Dark Web:** Ənənəvi axtarış sistemləri tərəfindən indekslənməyən və xüsusi proqram təminatları ilə daxil olunan şəbəkə. Tez-tez hakerlər və digər cinayətkarlar tərəfindən istifadə olunur.

# ƏHATƏ DAİRƏSİ

Bu siyasət, qurumun informasiya təhlükəsizliyinin qorunması məqsədilə təhdid kəşfiyyatına aid olan bütün fəaliyyətləri və prosesləri əhatə edir.

# MƏSULİYYƏTLƏR

Təhdid kəşfiyyatı siyasətinin effektiv həyata keçirilməsi üçün müxtəlif funksional qrupların və işçi heyətinin məsuliyyətləri aşağıdakı cədvəldə göstərilmişdir:

| **Funksiya/Qrup** | **Məsuliyyətlər** |
| --- | --- |
| **İnformasiya Təhlükəsizliyi Şöbəsi** | - Təhdid kəşfiyyatı strategiyasının hazırlanması və tətbiqi.  - Təhdid məlumatlarının toplanması, təhlili və qiymətləndirilməsi.  - Təhlükəsizlik insidentlərinə cavab tədbirlərinin əlaqələndirilməsi. |
| **İT Şöbəsi** | - Şəbəkə və sistemlərdəki təhlükəsizlik zəifliklərinin aşkarlanması və aradan qaldırılması.  - Texniki tədbirlərin həyata keçirilməsi. |
| **Rəhbərlik** | - Təhdid kəşfiyyatı ilə bağlı siyasət və prosedurların təsdiqlənməsi.  - Lazımi resursların ayrılması və nəzarətin təmin edilməsi. |
| **Bütün İşçilər** | - Təhdidlər barədə məlumatlı olmaq və müvafiq siyasət və prosedurlara riayət etmək.  - Şübhəli fəaliyyətləri vaxtında məlumatlandırmaq. |
| **Üçüncü Tərəf Təchizatçılar** | - Təhlükəsizlik tələblərinə riayət etmək və təhdid məlumatlarının paylaşılmasında iştirak etmək.  - Müqavilə şərtlərinə uyğun olaraq təhlükəsizlik insidentlərinə cavab vermək. |
| **Hüquq Şöbəsi** | - Təhdid kəşfiyyatı proseslərinin hüquqi və tənzimləyici tələblərə uyğunluğunu təmin etmək.  - Məlumatların məxfiliyinin qorunmasını təmin etmək. |

Bu cədvəl təhdid kəşfiyyatının qurum daxilində effektiv və strukturlaşdırılmış şəkildə həyata keçirilməsini təmin etmək məqsədilə məsuliyyət bölgüsünü dəqiq şəkildə təsvir edir.

# TƏTBİQ

## TƏHDİD KƏŞFİYYATININ İZAHI

Təhdid kəşfiyyatı, qurumun informasiya təhlükəsizliyinə təsir göstərə biləcək potensial təhdidlər barədə məlumat toplamaq, təhlil etmək və tədbir görmək prosesidir. Bu fəaliyyətlər, qurumun təhlükəsizlik zəifliklərini proaktiv şəkildə müəyyən etməsinə, riskləri azaltmasına və təhlükəsizlik insidentlərinə effektiv cavab verməsinə şərait yaradır.

Təhdid kəşfiyyatının əsas məqsədləri:

* Təhdidlərin potensial təsirini və yayılma ehtimalını qiymətləndirmək;
* Qurumun qərar qəbul etmə prosesini dəstəkləyəcək aktual və dəqiq məlumat təmin etmək;
* Zəifliklərdən istifadə etməyə çalışan təhdid aktyorlarının fəaliyyətlərini müəyyən etmək.

## TƏHDİD KƏŞFİYYATININ TƏBƏQƏLƏRİ

Təhdid kəşfiyyatı dörd əsas təbəqədə həyata keçirilir:

| **Təbəqə** | **Təsviri** | **Nümunələr** |
| --- | --- | --- |
| Strateji Kəşfiyyat | İnformasiya təhlükəsizliyinə təsir göstərə biləcək uzunmüddətli trendlərin və təhdidlərin təhlili | Sənaye trendləri, geopolitik risklər, kiber təhdid aktyorları ilə bağlı hesabatlar |
| Taktiki Kəşfiyyat | Təhdid aktyorlarının istifadə etdiyi metodlar, hücum texnikaları və zəifliklərin təhlili | Təhdid aktyorlarının TTP-ləri (taktikalar, texnikalar, prosedurlar), phishing hücumları |
| Əməliyyat Kəşfiyyatı | Qısamüddətli təhlükəsizlik insidentlərinin idarə edilməsi üçün aktual və detallı məlumatların təqdimatı | Zərərli proqramların analizi, hücum göstəriciləri (IOC), insident loglarının təhlili |
| Texniki Kəşfiyyat | Real vaxtda müəyyən edilmiş təhdidlərə sürətli cavab vermək üçün istifadə olunan texniki məlumatlar | Zərərli IP-lər, phishing domainlər, fayl hash-ləri, zəifliklər ilə bağlı texniki məlumatlar |

Hər bir təbəqə qurumun təhlükəsizlik üzrə qərarlarını dəstəkləmək üçün müxtəlif səviyyələrdə məlumat təqdim edir. Bu təbəqələr arasında əlaqələndirmə, təhdidlərin daha yaxşı başa düşülməsi və onlara qarşı müvafiq tədbirlərin hazırlanmasını təmin edir.

## QURUMDA STRATEJİ KƏŞFİYYAT

* İnformasiya Təhlükəsizliyi şöbəsi strateji kəşfiyyat fəaliyyətlərinin həyata keçirilməsinə cavabdehdir. Bu, kəşfiyyat məlumatlarının toplanması, analizi və nəticələrinin rəhbərliyə təqdim edilməsini əhatə edir;
* Kəşfiyyat prosesi üçün dəstək verən digər şöbələr arasında IT İnfrastruktur Şöbəsi, Risk İdarəetmə Şöbəsi və Hüquq və Uyğunluq Şöbəsi mövcuddur. Bu şöbələr, strateji kəşfiyyatın effektivliyini artırmaq üçün məlumatların toplanması və paylaşılmasına kömək edirlər;
* Qurumun strateji kəşfiyyat fəaliyyətlərinin uğurlu olması üçün, beynəlxalq və yerli qeyri-dövlət təşkilatları tərəfindən yayımlanan təhlükəsizliklə əlaqəli məlumatlar mütəmadi olaraq izlənməlidir;
* İTİS komandası izləniləcək təşkilatların siyahısını yaratmalı və bu siyahı İnformasiya Təhlükəsizliyi şöbəsi tərəfindən yoxlanılmalı, habelə izləniməlidir;
* Ehtiyac yarandığı zaman İnformasiya Təhlükəsizliyi şöbəsi yoxlanma və izlənmə prosesinə digər şöbələrin əməkdaşlarını təyin etməlidir.

## QURUMDA TAKTİKİ KƏŞFİYYAT

* İnformasiya Təhlükəsizliyi şöbəsi taktiki kəşfiyyatın həyata keçirilməsinə cavabdehdir və proses zamanı toplanan məlumatları İnformasiya Təhlükəsizliyi menecerinə təqdim edir;
* Ehtiyac olduğu təqdirdə Risk İdarəetmə Şöbəsi və IT İnfrastruktur Şöbəsi taktiki məlumatların toplanmasında və analizində İTİS Komandasına dəstək göstərməlidir;
* Taktiki kəşfiyyatın effektiv həyata keçirilməsi üçün məlumat toplama prosesinə xarici mənbələr (məsələn, beynəlxalq təhlükəsizlik təşkilatlarının yayımladığı təhlükə hesabatları, sektor üzrə yayılan insidentlər və tövsiyələr) və daxili resurslar (sistem logları, zərərli proqram analizləri) cəlb edilməlidir;
* Kəşfiyyat məlumatlarının izlənməsi üçün müvafiq mənbələr və əməkdaşlıq ediləcək tərəflərin siyahısını hazırlamalı və bu siyahını təsdiq üçün İnformasiya Təhlükəsizliyi şöbəsinə təqdim edilməlidir;
* Təhlükəsizlik təhdidlərinin taktiki analizində fokus aşağıdakılar üzərində olmalıdır:

1. Zərərli proqramların davranış təhlili;
2. Hücum göstəricilərinin (IOC) müəyyənləşdirilməsi və təhlili;
3. Təhdid aktyorlarının tipik davranışları və istifadə etdikləri texnikaların izlənməsi.

* **İnformasiya Təhlükəsizliyi şöbəsi** kəşfiyyat prosesindən əldə edilən məlumatların müntəzəm olaraq yenilənməsinə və uyğun tədbirlərin görülməsinə nəzarət etməlidir;
* Əldə edilmiş kəşfiyyat məlumatları əsasında, İT sistemlərinin müdafiəsini artırmaq məqsədilə proseslərə texniki dəyişikliklər və yeniliklər daxil edilməlidir. Bu dəyişikliklər **İT şöbəsi** tərəfindən həyata keçirilməli və İnformasiya Təhlükəsizliyi şöbəsinə hesabat təqdim olunmalıdır.

## QURUMDA ƏMƏLİYYAT KƏŞFİYYATI

* Əməliyyat səviyyəsində təhlükə mənbələrinin izlənməsi üçün xüsusi alətlərdən istifadə edilməlidir;
* Kəşfiyyat məlumatları “Dark Web” daxil olmaqla, digər riskli platformalarda aparılan axtarışlar nəticəsində əldə olunmalıdır;
* Əldə edilən məlumatlar Əməliyyat Təhlükəsizliyi Komandasına (ƏTK) göndərilməli və təhlil edilməlidir;
* Qurum sistemlərində mövcud zəifliklərin müəyyən edilməsi üçün müntəzəm təhlükəsizlik yoxlamaları həyata keçirilməli və İnformasiya Təhlükəsizliyi şöbəsi tərəfindən təhlil edilməlidir;
* Əməliyyat kəşfiyyatı çərçivəsində əldə edilən hər hansı təhlükə və zəiflik məlumatı əsasında dərhal operativ tədbirlər görülməlidir;
* Qurum daxilində istifadə olunan bütün monitorinq sistemlərindən (məsələn, SIEM, IDS/IPS) gələn alarmlar filtr edilməli və aidiyyəti üzrə müvafiq komandalara ötürülməlidir;
* Təhlükə və insident məlumatları üzrə təhlil tamamlandıqdan sonra uyğun cavab tədbirləri həyata keçirilməli və menecerə hesabat təqdim edilməlidir;
* Bütün əməliyyat kəşfiyyat məlumatları mütəmadi olaraq yenilənməli və aidiyyəti komandalar arasında paylaşılmalıdır;
* ƏTK-nin kəşfiyyat fəaliyyətlərinə uyğun olaraq əlavə resurslar tələb olunarsa, bu, təşkilati rəhbərlik vasitəsilə təmin edilməlidir.

## QURUMDA TEXNİKİ KƏŞFİYYAT

* Texniki kəşfiyyat çərçivəsində zərərli IP ünvanlar, domenlər, fayl hash-ləri və digər hücum göstəricilərinin (IOC) analizi həyata keçirilməlidir;
* Əldə edilən məlumatlar Texniki Təhlükəsizlik Komandasına (TTK) yönləndirilməli və təhlükəsizlik tədbirləri tətbiq olunmalıdır;
* Texniki sistemlər (SIEM, EDR, firewall-lar və digər təhlükəsizlik həlləri) vasitəsilə real vaxt rejimində məlumatlar izlənilməli və təhlil edilməlidir;
* Gələn alarmlar operativ olaraq İnformasiya Təhlükəsizliyi komandasına ötürülməlidir;
* Korporativ infrastrukturun zəiflikləri müəyyən edilməli və onların təsirini azaltmaq üçün texniki tədbirlər görülməlidir;
* Hücum göstəriciləri və digər texniki kəşfiyyat məlumatları təhlil edilərək aidiyyəti şöbələr və komandalara təqdim edilməlidir;
* Zərərli proqramların texniki analizi aparılmalı və nəticələr müvafiq komandalar ilə paylaşılmalıdır;
* Texniki kəşfiyyat fəaliyyətlərinə dəstək olmaq məqsədilə beynəlxalq və yerli təhlükəsizlik təşkilatlarından alınan məlumatlar izlənilməli və uyğun tədbirlər görülməlidir;
* Zəruri hallarda Texniki Təhlükəsizlik Komandası digər struktur bölmələrdən əlavə resurs və dəstək tələb edə bilər.

# ƏLAQƏLİ SƏNƏDLƏR

* ISO 27001:2022 Annex- 5.7

# İNTİZAM TƏDBİRLƏRİ

Siyasət təsdiq olunduğu gündən qüvvədədir. Siyasətdə qeyd olunan müddəaların pozulması halında Daxili Nizam İntizam Proseduru tətbiq olunacaq.

# SİYASƏTƏ NƏZARƏT

Siyasətə nəzarət hər il İT komitəsi tərəfindən həyata keçirilməlidir. Eyni zamanda, aşağıdakı hallarda da siyasət nəzərdən keçirilməlidir:

1. Qurumun strukturunda, iş proseslərində və ya informasiya resurslarında əhəmiyyətli dəyişikliklər baş verdikdə;
2. İnformasiya təhlükəsizliyi ilə bağlı rəhbərlik tərəfindən müəyyən edilən hədəflər və prioritetlər dəyişdikdə;
3. Qurumun fəaliyyət şəraiti, o cümlədən qanunvericilik və ya tənzimləyici tələblərdə dəyişikliklər olduqda;
4. İnformasiya təhlükəsizliyinin idarə olunması sahəsində yeni yanaşmalar tətbiq edildikdə.

# TƏSDİQETMƏ

Bu sənədi imzalamaqla, təqdim olunan məlumatların həqiqiliyini və düzgünlüyünü qəbul edirsiniz.

[vəzifə məlumatları]

[adı soyadı və ata adı]

\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_

[İmza] [Tarix]